

CLAIMS

WHAT IS CLAIMED IS:

1. A machine-executable method for executing a trusted command issued by a user, said method comprising the steps of:
  - (a) parsing the trusted command in an untrusted computing environment to generate a parsed command;
  - (b) submitting the parsed command to a trusted computing environment; and
  - (c) executing the parsed command in the trusted computing environment.
2. A method including the steps of claim 1 and additionally including the steps, executed after step (b) of claim 1, of:
  - (1) in the trusted environment, displaying a representation of the parsed command to the user;

1 (2) receiving a signal from the user signifying whether the  
2 displayed representation accurately represents the user's  
3 intentions;

4  
5 (3) if the signal signifies that the displayed representation does  
6 not accurately represent the user's intentions, then  
7 preventing the performance of step (c) of claim 1.  
8  
9

10  
11 3. The method of claim 2 wherein the representation of the parsed  
12 command is displayed, and the signal from the user is received,  
13 through a trusted path.  
14

15  
16  
17 4. The method of claim 1 wherein the trusted computing  
18 environment comprises a security kernel.  
19

20  
21  
22 5. The method of claim 1 wherein the untrusted computing  
23 environment comprises a general operating system.  
24

1  
2  
3 6. A method for executing in a computing system a trusted command  
4 issued by a user, said method comprising the steps of:

- 5
- 6 (a) receiving user identification data from the user via a  
7 trusted path;
- 8
- 9 (b) receiving the trusted command from the user via an  
10 untrusted path;
- 11
- 12 (c) parsing the trusted command in an untrusted computing  
13 environment to generate a parsed command;
- 14
- 15 (d) submitting the parsed command to a trusted computing  
16 environment;
- 17
- 18 (e) in the trusted computing environment, performing a security  
19 check on the parsed command and user identification data;  
20 and
- 21
- 22 (f) in the trusted computing environment, executing the trusted  
23 command.  
24



1  
2 9. A method including the steps of claim 6 and additionally including  
3 the steps, executed after step (d) and before step (f) of claim 6,  
4 of:

5  
6 (1) in the trusted environment, displaying a  
7 representation of the parsed command to a second  
8 user;

9  
10 (2) receiving a signal from the second user signifying  
11 whether the displayed representation accurately  
12 represents a legitimate command; and

13  
14 (3) if the signal signifies that the displayed  
15 representation does not accurately represent a  
16 legitimate command, then preventing the  
17 performance of step (f) of claim 6.

18  
19  
20  
21 10. A method for ensuring the existence of a trusted path in a  
22 computing system comprising the steps of:  
23

- 1 (a) in a trusted computing environment, upon login by a user, --  
2 assigning a process identifier to the user in the trusted  
3 computing environment;  
4  
5 (b) storing the assigned process identifier in trusted memory;  
6  
7 (c) establishing a trusted path;  
8  
9 (d) in the trusted path, displaying the process identifier to the  
10 user; and  
11  
12 (e) upon a subsequent entry into the trusted path, displaying  
13 the process identifier to the user.  
14  
15  
16  
17 11. The method of claim 10 wherein the process identifier is a  
18 randomly or pseudo-randomly generated group of alphanumeric  
19 characters.  
20  
21  
22  
23 12. The method of claim 11 wherein the process identifier is  
24 pronounceable.

20

15. A program storage device readable by a machine and tangibly embodying a representation of a program of instructions adaptable to be executed by said machine to perform the method of any one of claims 1 to 12.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
3  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23

- 61



1 18. Apparatus for controlling the execution by a machine of a trusted =  
 2 command that is issued by a user with user identification data and  
 3 that is parsed by untrusted parsing means to generate a parsed  
 4 command, comprising:

- 5
- 6 (a) trusted program storage means, readable by the machine,  
 7 for causing the machine to receive the user identification  
 8 data from the user;
- 9
- 10 (b) trusted program storage means, readable by the machine,  
 11 for causing the machine to receive the parsed command  
 12 from the untrusted parsing means;
- 13
- 14 (c) trusted program storage means, readable by the machine,  
 15 for causing the machine to perform a security check on the  
 16 parsed command and a security check on the user  
 17 identification data; and
- 18
- 19 (d) trusted program storage means, readable by the machine,  
 20 for causing the machine to execute the trusted command.  
 21  
 22  
 23

1 19. Apparatus as in claim 18 and additionally comprising:

2  
3 (1) trusted program storage means, readable by the machine,  
4 for causing the machine to display a representation of the  
5 parsed command to the user;

6  
7 (2) trusted program storage means, readable by the machine,  
8 for causing the machine to receive a signal from the user  
9 signifying whether the displayed representation accurately  
10 represents the trusted command; and

11  
12 (3) trusted program storage means, readable by the machine,  
13 for preventing the machine from executing the trusted  
14 command if the signal signifies that the parsed command  
15 does not accurately represent the trusted command.

16  
17 20. Apparatus as in claim 18 and additionally comprising:

18  
19 (1) trusted program storage means, readable by the machine,  
20 for causing the machine to display a representation of the  
21 parsed command to a second user;

22  
23 (2) trusted program storage means, readable by the machine,  
24 for causing the machine to receive a signal from the second

1 user signifying whether the displayed representation  
2 accurately represents a legitimate command; and

3  
4 (3) trusted program storage means, readable by the machine,  
5 for preventing the machine from executing the trusted  
6 command if the signal signifies that the parsed command  
7 does not accurately represent a legitimate command.

add  
a1